4

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,489	03/18/2004	Vincent J. Zimmer	42P18506	7634

7590 05/18/2007

Anthony H. Azure
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
VO, TED T	

ART UNIT	PAPER NUMBER
2191	

MAIL DATE	DELIVERY MODE
05/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,489	ZIMMER ET AL.	
	Examiner	Art Unit	
	Ted T. Vo	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7-12,15-19 and 21-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,7-12,15-19 and 21-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 03/05/07.

Claims 1-3, 7-12, 15-19, 21-23 are amended and claims 24-27 are new. The amendment necessitated new ground of rejections presenting in this action. Claims 1-3, 7-12, 15-19, 21-27 are pending in the application.

Specification

2. It should be noted that the content and arrangement of the specification does not comply with 37 CFR 1.77(b). Section headings should not be underlined. The specification should follow the guidelines. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase **"Not Applicable"** should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Particularly, the specification should include the section headings from (f) to (k). In this specification, the section headings should include (g) BRIEF SUMMARY OF THE INVENTION, or with the phase "**Not Applicable**" under the heading.

The specification of an application that does not comply with 37 CFR 1.77(b) would cause a **delay** when the application is apparently ready for allowance.

Response to Arguments

3. With regard to the argument under 101 issues, the amendment should be consistent to the specification. Applicants amended with "tangible machine-accessible medium"; however, therefore is no indication of "tangible machine-accessible medium" in the specification. The term "machine-accessible medium" in the specification remains **including propagated signals such as electrical, optical, acoustical or other form of propagated signals** (e.g., carrier waves, infrared signals, digital signals, etc.)

With regard to the argument to the claims rejected under 35 USC 102(a) are persuasive. Particularly, Applicants alleged that they have not found any reference to a computation or determination of a compound hash value based on a first and a second virtual hash value. The referenced section of Garfinkel discusses establishing trust by using two certificate chains to show that a VM with a particular hash is running and that the hash represents a particular version of a particular software program (see second full paragraph, p. 196). Garfinkel discloses verifying one or more hash numbers in the attestation process, however, Garfinkel does not disclose, "determining a compound hash value..." and "storing the compound hash value in a trusted hardware device shared between the first and second VM using the VMM multiplexer." See also page 14 of the Applicants' specification for the security benefits associated with the use of a compound hash value.

Examiner responds: See the reference, p. 196, right col., all paragraphs, every VM is included with "VM's hash", and the verifications of 1, 2, 3, etc. With regard to the TERRA architecture

(Figure 1: Attestation, Sealed Storage device), TERRA allows multiple VMs running independently and concurrently. TERRA uses "Attestation, Sealed Storage device" in Figure 1 to store a compound of the hash values of VM's run under TERRA. For example, See sec. 2.2, start at p. 195, particularly, second paragraph in left col., of p. 196, SHA-1, generates and signs a certificate containing (1) a SHA-1 hash of the attestable parts of the higher-level component, and (2) the higher level component's public key and application data. This certificate binds the public key to a component whose hash is given in the certificate.

The amendment fails to point out patentability according to 1.111(c), but argued only non patentable features which are already accomplished in public domain.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. The claims 12, 15-18 are rejected under 35 U.S.C 101 because the claimed invention is directed to non-statutory subject matter.

A claimed invention as a whole must accomplish a practical application. That is, it must produce a **"useful, concrete and tangible result"** State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02. Media which are wireless, forms of energy, signals are not **concrete and tangible**.

As per Claims 12, 15-18: Claims 12, 15-18 recite an article of manufacture comprising a tangible machine-accessible medium (not defined in the specification).

> The term "tangible machine-accessible medium" is not consistent to the specification, this term is contrast to descriptions in the specification, i.e., "machine-accessible medium" in the specification remains **including propagated signals such as electrical, optical, acoustical or other form of propagated signals** (e.g., carrier waves, infrared signals, digital signals, etc.)

Claims 12, 15-18 fail to meet the statutory claims under 35 U.S.C 101 because the specification defines the medium having carrier waves, infrared signals, digital signals, etc.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-3, 7-12, 15-19, 21-27 are rejected under 35 U.S.C. 102(a) as being anticipated by Garfinkel et al., "Terra: A Virtual Machine-Based Platform for Trusted Computing", ACM, 2003.

Given the broadest reasonable interpretation of followed claims in light of the specification.

As per Claim 24: Garfinkel discloses,

A method, comprising:

loading a virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer (see p.194, left col., last paragraph, "allow many virtual machines (VMs) to run...": *plurality of virtual machines*. See Figure 1, TVMM: "VMM": i.e., TVMM is loaded in a hardware platform)*;* ***loading a first and a second virtual machine (VM) supported by the VMM*** (See sec. 2, p. 194, TERRA allows multiple VMs running independently and concurrently, e.g., see left col., last paragraph of p. 194. See p. 196, left col., third paragraph);

and sharing a trusted hardware device between the first VM and the second VM using the VMM multiplexer (refer TVMM, T: trusted; see p. 194, right col., last paragraph, "multiplex").

As per Claim 25: Garfinkel discloses, *The method of claim 24 wherein the VMM is loaded from firmware, the firmware including instructions compliant with an Extensible Firmware Interface (EFI) specification*

(See sec. 2.2, p.195-196, and p. 199, e.g., "firmware", "VM firmware", and see p.195, left col. Extensibility).

As per Claim 26: Garfinkel discloses, *The method of claim 1 wherein sharing the trusted hardware device comprises multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer* (See p. 194, right col., last paragraph, "multiplex", also see Figure 1).

As per Claim 27: Garfinkel discloses, *The method of claim 24 further comprising:*

determining a first VM platform configuration including a first hash value based on information measured from the first VM and a second VM platform configuration including a second hash value based on information measured from the second VM;

using a trusted hardware device shared between the first and the second VM to determine a compound hash value based on a combination of the first VM platform configuration and the second VM platform configuration (See Figure 1: Attestation, Sealed Storage device. TERRA allows multiple VMs run independently and concurrently. TERRA uses "Attestation, Sealed Storage device" in figure 1 to store a compound of the VM's hash values. For example, See sec. 2.2, start at p. 195, particularly, second paragraph in left col., of p. 196, SHA-1, generates and signs a certificate containing (1) a SHA-1 hash of the attestable parts of the higher-level component, and (2) the higher level component's public key and application data. This certificate binds the public key to a component whose hash is given in the Certificate)*; and*

storing the compound hash value in the trusted hardware (See p. 200, sec. 4.6, Sealed Storage).

As per Claim 1: Garfinkel discloses,

A method, comprising:

loading a virtual machine monitor (VMM) to support a plurality of virtual machines in a computer system, the VMM including a VMM multiplexer (see p.194, left col., last paragraph, "allow many virtual machines (VMs) to run...": *plurality of virtual machines*. See Figure 1, TVMM: "VMM": i.e., TVMM is loaded in a hardware platform)*;*

loading a first and a second virtual machine (VM) supported by the VMM (p.194, left col., last paragraph, 'allow many virtual machines'; p. 196, left col., third paragraph);

determining a first VM platform configuration including a first hash value based on information measured from the first VM and a second VM platform configuration including a second hash value based on information measured from the second VM (See p. 196, right col., all paragraphs, every VM is included with "VM's hash", the verifications of 1, 2, 3, etc.);

using a trusted hardware device shared between the first and the second VM to compute a compound hash value (Figure 1: Attestation, Sealed Storage device. TERRA allows multiple VMs run independently and concurrently. TERRA uses "Attestation, Sealed Storage device" in figure 1 to store a compound of the VM's hash values. For example, See sec. 2.2, start at p. 195, particularly, second paragraph in left col., of p. 196, SHA-1, generates and signs a certificate containing (1) a SHA-1 hash of the attestable parts of the higher-level component, and (2) the higher level component's public key and application data. This certificate binds the public key to a component whose hash is given in the certificate) ***based on a combination of the first VM platform configuration including the first hash value and the second VM platform configuration including the second hash value*** (See Figure 1, interface section between TVMM and hardware platform, the and see sec. 4.4, start at p. 199); ***and storing the compound hash value in the trusted hardware device*** (See p. 200, sec. 4.6, Sealed Storage).

As per Claim 2: Garfinkel discloses, *The method of claim 1 wherein the VMM is loaded from firmware, the firmware including instructions compliant with an Extensible Firmware Interface (EFI) specification* (See sec. 2.2, p.195-196, and p. 199, e.g., "firmware", "VM firmware", and see p.195, left col. Extensibility).

As per Claim 3: Garfinkel discloses, *The method of claim 1 wherein sharing the trusted hardware device comprises multiplexing a first request from the first VM and a second request from the second VM to the trusted hardware device using the VMM multiplexer* (See p. 194, right col., last paragraph, "multiplex", also see Figure 1).

As per Claim 7: Garfinkel discloses, *The method of claim 1, further comprising sealing secret information from the first VM with the compound platform configuration using the trusted hardware device* (Refer to

Terra's signatures such as seal storage in Figure 1, and see p. 195, left col., full sec. 2.1, "trusted platform", and see whole sec. 4.5, Device Driver Security).

As per Claim 8: Garfinkel discloses, *The method of claim 7, further comprising unsealing the secret information using the trusted hardware device if a current first VM platform configuration matches the first VM platform configuration* (See p. 195, left col., full sec. 2.1, "trusted platform", and see whole sec. 4.5, Device Driver Security).

As per Claim 9: Garfinkel discloses, *The method of claim 1, further comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware requests sent to the trusted hardware device from the first VM and the second VM* (the operation of Figure 1).

As per Claim 10: Garfinkel discloses, *The method of claim 9, further comprising reporting a first request from the first VM is in progress when the trusted hardware device is polled by the first VM regarding the status of the first request, the first request actually waiting in the queue to be processed by the trusted hardware device* (the operation of Figure 1).

As per Claim 11: Garfinkel discloses, *The method of claim 1 wherein the trusted hardware device includes a trusted platform module (TPM)* (Figure 1, with sealed storage device).

As per Claim 12: Garfinkel discloses claim 12. See the rationale addressed in Claim 1.

As per Claim 15: Garfinkel discloses, *The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising sending a seal command to the TPM to seal secret information from the first VM with the compound hash value* (The operation of Figure 1, sealed storage device, see p. 196, right col., all paragraphs, "VM's hash").

As per Claim 16: Garfinkel discloses, *The article of manufacture of claim 15 wherein execution of the plurality of instructions further perform operations comprising sending an unseal command to the TPM from the first VM to unseal secret information associated with the first VM* (The operation of Figure 1, sealed storage device, see p. 196, right col., all paragraphs, "VM's hash").

As per Claim 17: Garfinkel discloses, *The article of manufacture of claim 12 wherein execution of the plurality of instructions further perform operations comprising maintaining a TPM request queue to queue*

a first TPM request from the first VM and a second TPM request from the second VM. (The operation of Figure 1).

As per Claim 18: Garfinkel discloses, *The article of manufacture of claim 17 wherein execution of the plurality of instructions further perform operations comprising reporting the second TPM request is in progress if the TPM is polled by the second VM, the second TPM request actually waiting in the TPM request queue* (the operation of Figure 1).

As per Claim 19: Garfinkel discloses claim 19, see rationale addressed in Claim 1.

As per Claim 21: Garfinkel discloses, *The computer system of claim 19 wherein execution of the plurality of firmware instructions further perform operations comprising maintaining a queue of trusted hardware device requests by the VMM multiplexer, the trusted hardware device requests sent to the trusted hardware device from the first VM and the second VM.* See rational in the rejection of Claim 9.

As per Claim 22: Garfinkel discloses claim 22, see rationale addressed in Claim 1. *The computer system of claim 19 wherein the firmware instructions compliant with an Extensible Firmware Interface (EFI) specification* (see p.195, left col. Extensibility).

As per Claim 23: Garfinkel discloses claim 23, see rationale addressed in Claim 11.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ted T. Vo whose telephone number is (571) 272-3706. The examiner can normally be reached on 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wei Y. Zhen can be reached on (571) 272-3708.

The facsimile number for the organization where this application or proceeding is assigned is the Central Facsimile number **571-273-8300**.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TTV
May 11, 2007

TED VO
PRIMARY EXAMINER